أمن نظم المعلومات

عمل الطالب :سامي عامر جبر

المحاضرة الاولى

Why we need information security??

- **Information security is important for several reasons :**
- **1 - protection of confidentiality.**

  Infosec ensures that sensitive data remains confidential and is a accessible only to authorized people.
- **2 - preservation of integrity.**

  Infosec measures prevent authorized modification, delete of data.
- **3 - Availability:**
- infosec ensures that data and information are available to authorized users whenever needed. this involves implementation measures to prevent service disruptions system fuelers or cyberattack that could result in downtime or unavailability of critical resources.

- **4 - Protection againts.**

  Cyber theuts such as malware, phishinfg attack, etc.

- **5 - business continuity.**

  Infosec is important for ensuring the continuity of business operations particularly in the face of unexpected events such as natural disasters.

- **6 - protection of intellectual property.**

  Infosec helps safeguard intellectual properity, trade secrets from thef, unauthorized access.

- **Computer data protection methods :**

1- encryption.

2 - data backup.

3 - educate employee.

4 - using antiviruses.

5 - firewall.

6 - biomitric_method.

- **Computer security :**

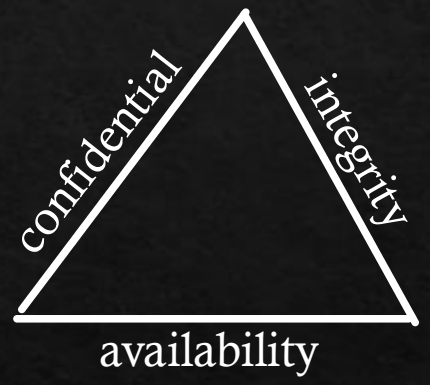
  Means keeping computer system safe.

  this includes protections everything like computer itself the software out it, the data it hold.

  and how to connects to other devices.

المحاضرة الثانية

- **Three main goals that are central of computer security (C.I.A) :**



- **Confidentiality :**

  Measures keeping safe and only sharing it with authorized people, protecting privacy data.

- **Integrity :**

  Means making sure info stays correct and safe being changed or deleted.

- **Availability :**

  Means making sure is always accessible and can be used when needed.

- **Computer & network can present challenges for several reasons :**

1 – At first security might seem simple but keeping everything safe can get complicated.

2 – When making things secure, we should think about the different ways someone's might to try to break it.

3 – Keeping info safe is like a strategic game between people trying to break in and those trying to keep them out attackers only need to find one weak spot, but defenders must find all the places where someone could get it.

4 – The important of security measures might not fully understand until there is a security breach.

5 – Security is often seen as something to think about later instead of being part of the original for a system.

6 – Keeping things secure usually means using complicated rules and protecting important info which makes things even more complicated.

المحاضرة الثالثة

- **Security attacks:**

Type of attacks in infosec in the domain of infosec, attacks are generally classified into 2 main categories :

1- Passive attack :

These involves silently monitoring or ears dropping on data transmissions together info without altering system resource.

A common type include :

a - Msg contents exposure.

2 - Active attack :

These entail actively modifying data streams.

Example of active attack :

a - Identity theft : pretending to be someone else to gain unauthorized access.

b - Msg altering.

c - Dos attack : denial of service.

Ex : overloading networks to hinder normal communications.

Example of threats in infosec :

1 – Frand and theft :

* - people who should not get (unauthorized) in might try to steal many of into ur system.

* - This could be done by people inside the organization and outsiders.

* - Former employees who still have access to system to system can also be a threat in their access isn't stopped quickly.

* - Social engineering :

Social engineering tricks people into breaking security rules and sharing secret info.

it can happen over the phone, or online.

often using fake email or files with harmful software.

2 – Insider threats.

3 – Malicious, hackers :

Reasons can be different from wanting excitement to wanting money.

المحاضرة الرابعة

- **Malicious code :**

  This refers to harmful software like viruses, trojan horse, worms, and logic bombs.

1 - Virus : Copy them self and attack to other programs.

2 - Trojan horse : Do what you want but also have harmful.

3 - Worms : copy them self and spread though network.

4 - Logic bombs : do harmful things at a certain time or when certain things happen.

5 - Ransomware : Ransomware stop you from using system until you pay money, either by locking your files.

- **Security services include 6 main categories :**

  1 - Authentication.

  2 - Access control.

  3 - Data confidentiality.

  4 - Integrity.

  5 - Non-repudiation : this prevent people from dinging they sent or received a msg.

  6 - Availability.

- **Security mechanism:**

  Are tools used in communication protocol to ensure data digits signature for verifying data integrity.

- **Cybersecurity threats :**

  1 – Virus Hoax :

  A virus hoax is false warning about a computer virus that does not actually exist.

  2 – Backdoor :

  Is a secret method used by hacker to gain unauthorized access to a computer system.

  3 – Brute force attack.

  4 – Man-in-the middle attack.

المحاضرة الخامسة

- **To make a service secure we need to :**

  1 – Secure msg transformation, we use encryption to scramble msg, so only authorized people can understand them. Encryption turns msg into a secret code that’s needs a special key to unlock.

  2 – Make secret info safely, we create secret info likes keys or passwords in a secure way to stop unauthorized access.

  3 – Shared secrets securely : After making secret info, we shared it securely between parties we use methods like secure channel or protocols to ensure it's only seen by the right people.

  4 – Design a safe plan : we create a set of rules and stops for sending msg. Securely, this plan include encryption, authentication and ways to handle errors. Popular protocols like TLS (transport layer security) or SSH (secure shell) help with this.

- **Modular arithmetic :**

Classical encryption techniques.

---

1 – Symmetric. (one key).

2 – Asymmetric. (two key).

---

* – **plain text :** original text.
* – **Encryption algorithm :** performs various substitutions and transformation on the plaintext.
* – **Secret key :** is like a special code used during encryption.
* – **Ciphertext :** this is the scrambled msg. Produced as output depends on the plaintext and the secret key.
* – **decryption algorithm :** reversing the encryption process you start with encryption msg (ciphertext) and the secret key, and you use then to restore the original msg (plaintext).

المحاضرة السادسة

- **Ensuring safe encryption important steps :**

  1 – Strong encryption method :

  Like (AES)

  2 – Keeping the secret key safe :

  both the sender & receiver must get the secret key in the safe way and make sure it's stay secret.

- The encryption algorithm turns msg (x) and key (k) into ciphertext (y).

  x = d (k , y)

- Cryptography: is the practice of security communication by encoding & decoding info, Aiming to maintain confidentiality, integrity, and authentication of data.

- **Cryptographic system differ based on three main factors :**

p : plaintext

c : cyphertext

1 - The type of operations : used for transforming (p) to (c)

Encryption algorithm : typically involves substitution (replacing element) and transposition (rearranges element) to convert (p) to (c).

2 - Number of keys : used in both sender & receiver use the same key the system in related to as symmetric, single key, secret key, private key.

If the sender & receiver use deferent keys the system is referred to as asymmetric, two key, or public key encryption.

3 - The way in which the (p) is processed : in cryptography, the processing of the plaintext can be categorized

Into z main method: **...**

…

A – Block cipher :

This method process input data in fixed-size (AES) Hello world!.

B – Stream cipher :

Encryption & decryption one element at a time byte/bit.

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

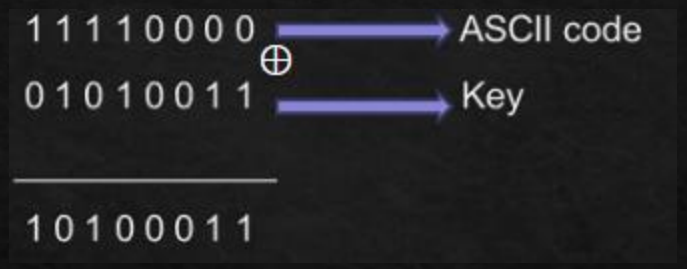
المحاضرة السابعة

Example for stream :

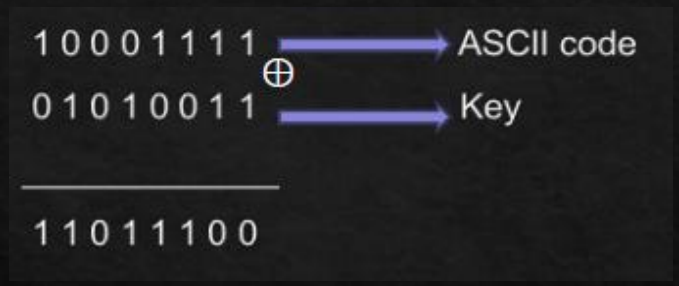
Word : HI

Key : 01010011

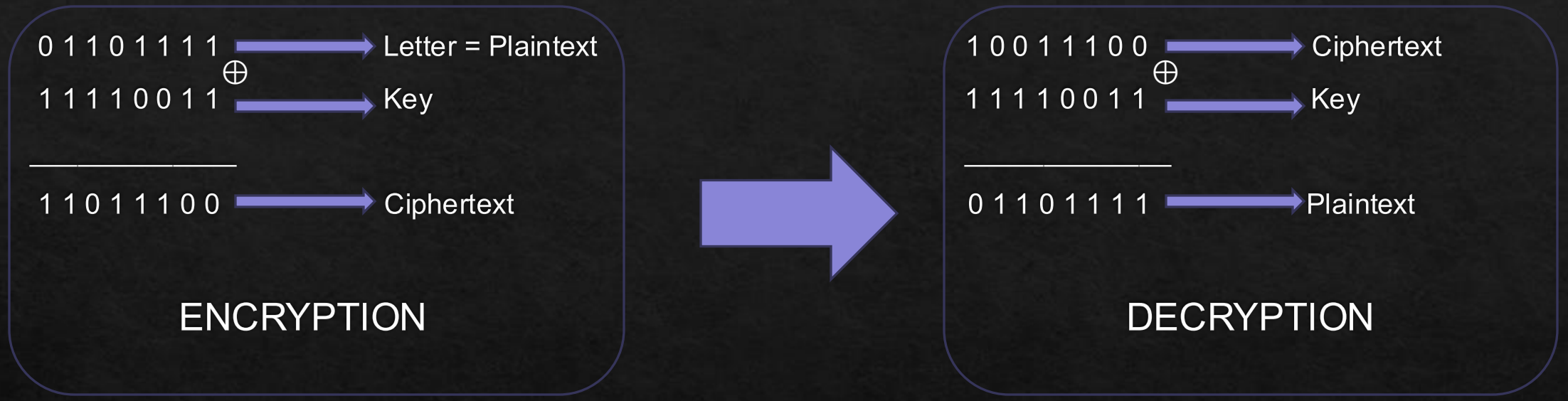
H =



I =



The final answer = 10100011 11011100



- **Cryptoanalysis :**

  involves using the characteristic of the algorithm and sometimes info about the plaintext-ciphertext pairs to try to figure out the msg or key.

- Symmetric & Asymmetric cryptosystem :

  Symmetric :

Fig(1) : symmetric

Use the same key for encryption and decryption such as AES, DES

Asymmetric :

Fig(2) : Asymmetric

- **Substitution techniques :**

Substitution : replaces plaintext element with others,

Like :

Caeser cipher : each letter of the alphabet is moved three positions forwards.

$$C = E(K) = (P+K) \bmod 26 \quad \text{(where } K = 3\text{)}$$

For decryption : $P = D(K,C) = (C - K) \bmod 26$

Example : Do the encryption for word (HELLO)

	H	E	L	L	O
Alphabatic number ←	7	4	11	11	14
Shifting 3 ←	3	3	3	3	3 +
	---	---	---	---	---
ciphertext ←	10	7	14	14	17
	K	H	O	O	R

HELLO → KHOOR

المحاضرة الثامنة

- **Monoalphabetic cipher :**

  Is a substitution cipher when each letter in the plaintext is consistently replaced by the same letter as symbol in the ciphertext.

  Ex):

  Encrypt the msg "ITEM" key: EYFQWDTCRJBGANXOILZMPSHKVU

A	B	C	D	E	F	G	H	I	J	K	L	M
(E)	(Y)	(F)	(Q)	(W)	(D)	(T)	(C)	(R)	(J)	(B)	(G)	(A)
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(N)	(X)	(O)	(I)	(L)	(Z)	(M)	(P)	(S)	(H)	(K)	(V)	(U)

answer : RMWA * Decryption -----> عملية عكسية

- Keyword cipher :

  * - specific word

  * - specific letter

A keyword cipher is a form of monoalphabetic substitution.

من غير تكرار للأحرف

Ex):

Specific word : mathematics Letter : F word : HELLO

From here we start

A	B	C	D	E	F	G	H	I	J	K	L	M
(V)	(W)	(X)	(Y)	(Z)	(M)	(A)	(T)	(H)	(E)	(I)	(C)	(S)
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(B)	(D)	(F)	(G)	(J)	(K)	(L)	(N)	(O)	(P)	(Q)	(R)	(U)

Answer : HELLO -----> TZCCD

- Keyword cipher :
  1 – Select keyword.
  2 – Write msg.
  3 – Write keyword length msg.
  4 – Add.

Ex) :

Select keyword = "CIPHER" Msg : "meet me to night"

12	4	4	19	12	4	19	14	13	8	6	7	19
M	E	E	T	M	E	T	O	N	I	G	H	T
2	8	15	7	4	17	2	8	15	7	4	17	2
C	I	P	H	E	R	C	I	P	H	E	R	C

+

*) If word length more than 25, we make mod 26

14	12	19	26	16	21	21	22	27	15	10	24	21
O	M	T	A	Q	V	V	W	C	P	K	Y	V

Answer : OMTAQVVWCPKYV

المحاضرة التاسعة

- **Frequency analysis :**

  Cryptography, relative letter frequencies aid in deciphering encrypted Msg by identifying common patterns facilitating code-breaking for

  Ex : in English "e" and "t" are common while "z" and "q" are rare.

Ex): use frequency analysis to decrypt this ciphertext :

Ciphertext : WKLVPHVVDJHLVWRSVHFUHW

repetition of letters in ciphertext : W=3, K=1, L=2, V=5, P=1, H=4, D=1, J=1, R=1, S=1, F=1, U=1

The most letter frequent letter

Key : (V – E) = (21 – 4) = 17 — the key = 17

The most common letter — alphabetical order

	W	K	L	V	P	H	V	. . .
	22	10	11	21	15	7	12	. . .
–	17	17	17	17	17	17	17	. . .
	5	19	20	4	24	16	4	. . .

This is not understood, we take the letter with the highest second repetition, which is "H".

Key (2) : (H – E) = (7 – 4) = 3 the key is = 3

W	K	L	V	P	H	V	V	D	J	H	L	V	W	R	S	V	H	F	U	H	W
22	10	11	21	15	7	21	21	3	9	7	11	21	22	17	19	21	7	5	20	7	22
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

–

19	7	8	18	12	4	18	18	0	6	4	8	18	19	14	15	18	4	2	17	4	19
T	H	I	S	M	E	S	S	A	G	E	I	S	T	O	P	S	E	C	R	E	T

The word is : "this message is top secret"

- **Playfair cipher :**

  The Playfair cipher, famous for encoding multiple letter combination operators by treating pairs of letters in the plaintext as singular units and transforming them into ciphertext diagram, this method relies on a 5x5 matrix of letters generated using a keyword.

- **The encryption process follows these rules of plaintext pairs :**

  1 – repeated letters within a pair are separated by filler letter.

  For example : "balloon" becomes (ba lx lo on)

  2 – if both plaintext letter are in the same row each is replaced by the letter to its right,

  With circular wrapping at the end of the row for instance "ar" becomes "RM".

3 – when both letters fall in the same column, each is substituted by the letter down with circular wrapping at the top of the column, for ex: "Mu" becomes "cm".

4 – otherwise each plaintext letter in the pair is replaced by the letter in its own row and the column occupied by the other plaintext letter

Ex: "Hs" becomes "BP" and "EA" becomes "IJM".

- Polyalphabetic cipher :

  In a polyalphabetic cipher different substitution rules are used within the
  The same msg, this means that different alphabets or substitution patterns
  May be applied based on a key or some other mechanism.

- Polyalphabetic cipher :

  In a polyalphabetic cipher different substitution rules are used within the the same msg, this means that different alphabets or substitution patterns may be applied based on a key or some other mechanism.

Ex) : msg="SECURITY"

key is a rules : key 1 : shift first letter 3 position to right.

key 2 : shift first letter 5 position to right.

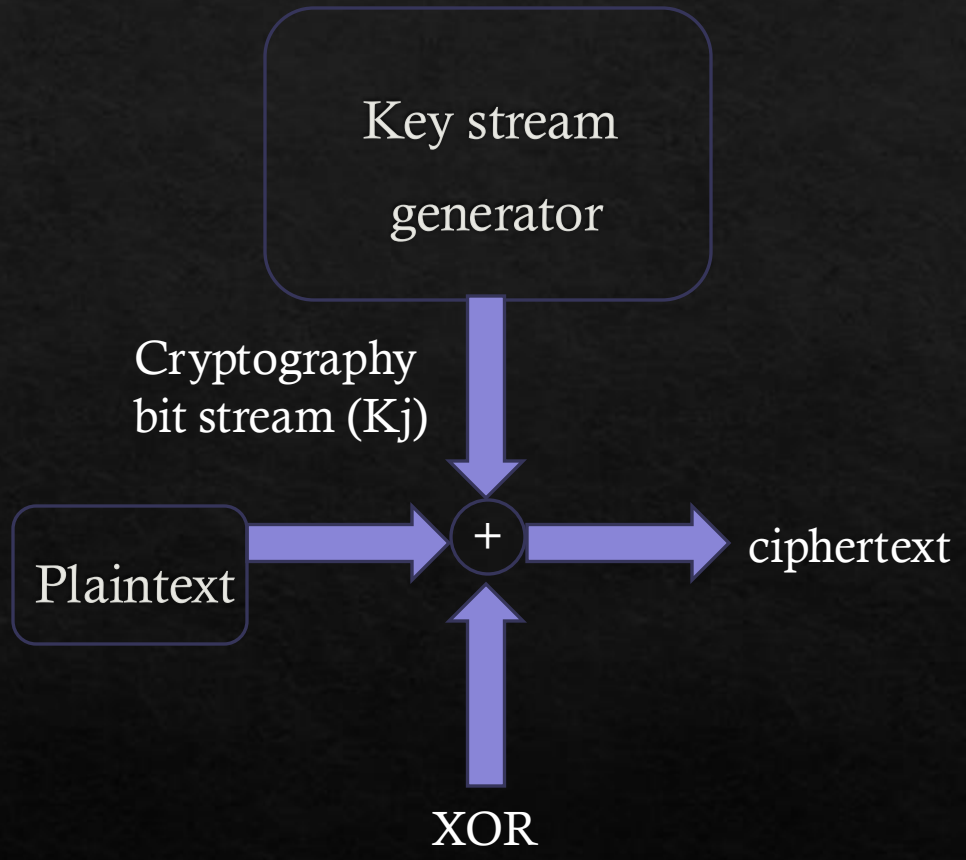
key 3 : shift first letter 7 position to right. (if the third letter is not present we don't make the rule)

S E C	U R I	T Y
S+3 = V	U+3 = X	T+3 = W
E+5 = J	R+5 = W	Y+5 = D
C+7 = J	I+7 = P	_

Answer : VJJXWPWD

Decrypt : عملية عكسية

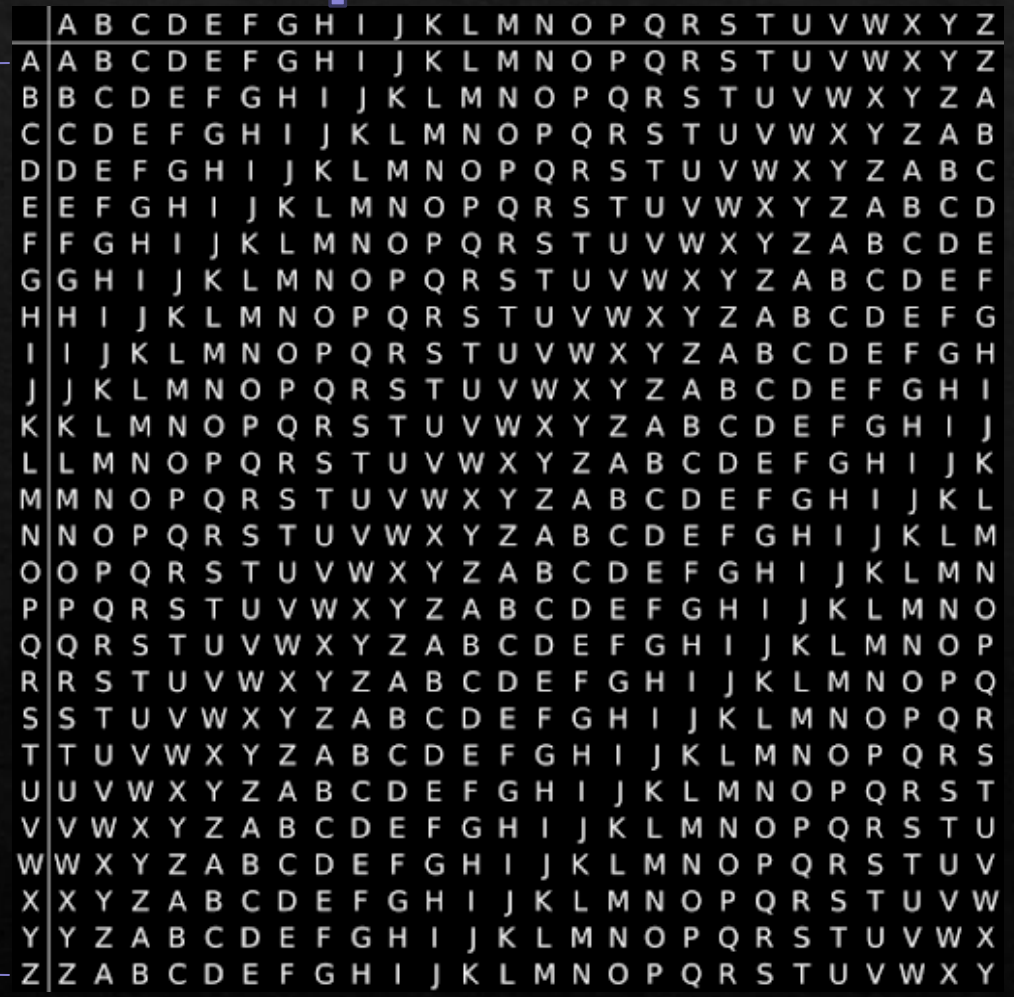
- **Vernam cipher :**



- **Vigener cipher** : it's a simple form of monoalphabetic.

plaintext

key



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ex : key = "AD"

Plaintext = "hi"

Answer : "HL"

- **Transposition cipher :** Row transposition permutation.

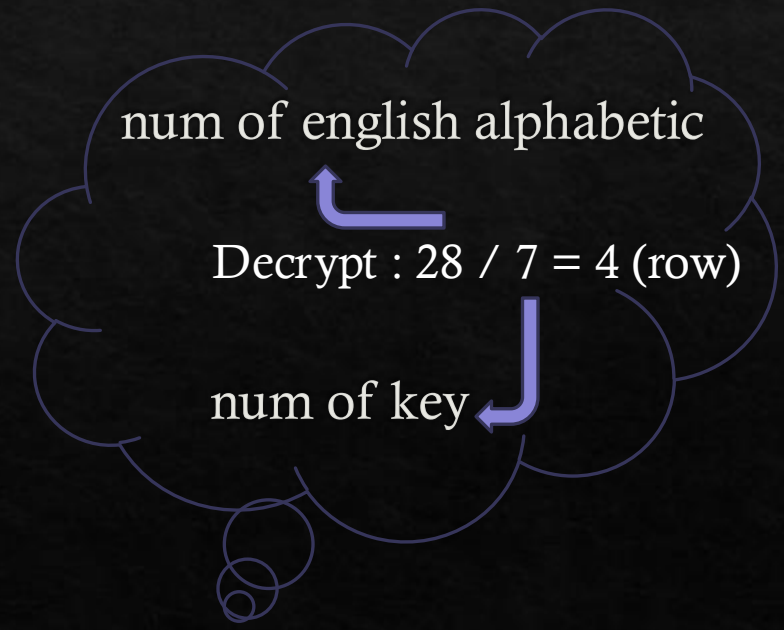
Ex) :

plaintext = "ATTACK POSTPOND UNTILL TWO AM".

KEY = "4312567"

4	3	1	2	5	6	7
A	T	T	A	C	K	P
O	S	T	P	O	N	D
D	U	N	T	I	L	L
T	W	O	A	M	x	x

Answer : TTNO APTA TSUW AODT COIM KNLx PDLx



محاضرة الثانية عشر

- Hill cipher : use matrix to encrypt and decrypt modular arithmetic.

  For (a) mod (b) divide (a) by (b) and take the remainder.

  - Modular inverse :

    For mod m

    $= (a * a^{-1}) \bmod m = 1$

A	1	3	5	7	9	11	15	17	19	21	23	25
A^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

- Ex) : Encrypt Msg = "HELLO WORLD"

  By Hill cipher whin Key = $\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$

$$\begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} * \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 14+4 \\ 21+16 \end{pmatrix} = \begin{pmatrix} 18 \\ 37 \end{pmatrix} \rightarrow \begin{pmatrix} 18 \\ 11 \end{pmatrix} = \begin{pmatrix} S \\ L \end{pmatrix}$$

after mod 26

$$\begin{pmatrix} L \\ L \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \end{pmatrix} * \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 7 \\ 25 \end{pmatrix} = \begin{pmatrix} H \\ Z \end{pmatrix}$$

$$\begin{pmatrix} O \\ W \end{pmatrix} = \begin{pmatrix} 14 \\ 22 \end{pmatrix} * \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 24 \\ 0 \end{pmatrix} = \begin{pmatrix} Y \\ A \end{pmatrix}$$

$$\begin{pmatrix} O \\ R \end{pmatrix} = \begin{pmatrix} 14 \\ 17 \end{pmatrix} * \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 19 \\ 6 \end{pmatrix} = \begin{pmatrix} T \\ G \end{pmatrix}$$

$$\begin{pmatrix} L \\ D \end{pmatrix} = \begin{pmatrix} 11 \\ 3 \end{pmatrix} * \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 25 \\ 19 \end{pmatrix} = \begin{pmatrix} Z \\ T \end{pmatrix}$$

Answer = SLHZYATGZT

Decrypt :

$$\frac{1}{\text{Det (k)}} * \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

(المثال موجود بالدفتر)